UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/676,499	09/30/2003	Theodore C. Tanner JR.	MS1-1349US	8575

22801 7590 12/08/2010

LEE & HAYES, PLLC
601 W. RIVERSIDE AVENUE
SUITE 1400
SPOKANE, WA 99201

EXAMINER	
GELAGAY, SHEWAYE	
ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
12/08/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

lhptoms@leehayes.com

Office Action Summary	Application No.	Applicant(s)	
	10/676,499	TANNER ET AL.	
	Examiner	Art Unit	
	SHEWAYE GELAGAY	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09/20/10*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-9,11-22 and 46-64* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-9,11-22 and 46-64* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application.
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to the Amendment filed on 09/20/10.

2. Claims 1, 46, 49 and 52 have been amended.

3. Claims 1, 3-9, 11-22 and 46-64 are pending.

Response to Arguments

4. Applicant's arguments filed on 09/20/10 have been fully considered but they are not persuasive.

5. With respect to the rejection of claims 1, 3-7, 46, 49 and 52 are rejected under 35 U.S.C. 101, the applicant argued that "According to the specification [0136], a "computer storage medium" is described in this manner: "Computer storage media" include volatile and non-volatile, removable and non-removable media implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules, or other data. Computer storage media includes, but is not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which may be used to store the desired information and which may be accessed by a computer. This description appears to include only statutory subject matter. " Examiner would like to point out that a computer readable storage media as described above is not limited to a statutory subject matter. The specification does not explicitly define the computer readable storage media but gives. A computer storage

media can be broadly interpreted as being a signal or transmission type media that does not fall within statutory subject matter. Therefore, claims 1, 3-7, 46, 49 and 52 are directed to non-statutory subject matter under 35 U.S.C. 101. Examiner suggests amending the claims to include "non-transitory computer storage medium" to overcome this rejection.

With respect to the rejection of claims 1, 4-9, 12-18, 20-22 and 48-52 under 35 U.S.C. 103:

The Applicant argued that "Lenoir describes an approach for achieving less expensive watermark detection by utilizing existing available memory on a multimedia device but external from the watermark detector itself. Unlike the claim language about the reception of subject input stream, Lenioir is focused on actions related to data that is already received and stored in memory." Examiner respectfully disagrees. Claims are to be given broadest reasonable interpretation, Examiner would like to point out that phrase like "***observing and determining" "intervening with clear reception"*** and ***"subject input stream***" are broadly interpreted. Claim 1 merely recites "observing and determining a location in a processor-readable memory of a computer, where watermark detector receives subject input stream; and intervening with clear reception the input stream.

The Applicant argued that "According to Lenoir, its watermark detector processes the data stored in the buffer. However, to do that presumably the watermark detector must still receive data in order to process it. The data stored in Lenoir buffer has not been received by the Lenioir's watermark detector. Therefore, Lenior fails to teach

"observing and determining a location in a processor-readable memory where [the watermark detector] receives a subject input stream." Examiner respectfully disagrees. The specification on paragraph [0058]-[0060], describes "content producer/provider that produces original content and distributes content over a network to the computer client or via processor-readable media such as CD_ROM. .. stores the watermarked intangible goods onto processor-readable media." Lenoir teaches integrity and confidentiality problem, are observed when watermark detectors share memory resources. A hacker wanting to obstruct the watermark detection function could replace the data stored by the detector through zeroes or dummy data before it is retrieved again by the detector. Furthermore a hacker could glean information about the precise shape of the watermark by studying the data stored in the external memory. Lenoir teaches to improve the security of outsourcing of intermediate results during a watermark detection process. A watermark detector 4 would typically be integrated with the block decoder 3. The watermark detector 4 typically collects some video or audio material in buffer 5, performs some signal processing on this buffer 5, correlates the contents of the buffer 5 with a watermark and performs some further signal processing. The usage of the buffer 5 makes the system vulnerable to attacks by a hacker. The hacker could try to destroy or manipulate the intermediate results stored in buffer 5 in a way that is advantageous to him. (i.e. observing and determining a location in a processor-readable memory of a computer, where watermark detector receives a subject input stream) Furthermore, the correlation of the content of the buffer 5 with watermark is also very sensitive to attacks in which a hacker wants to learn any

information from the intermediate result in order to gather information about the watermark, since after the correlation some information about the watermark is contained in the buffer 5.

Applicant further argued that "As shown in Fig. 1 of Lenoir above and described at col. 4, lines 1-18, the watermark detector 4 is integrated with the block decoder 3. Buffer 5 is separate from the watermark detector 4. Lenioir's watermark detector operates on data stored in the separate buffer. "The watermark detector 4 typically collects some video or audio material in the buffer 5, performs signal processing on this buffer 5, correlates the contents of the buffer 5 with watermark and performs some further signal processing." Applicant argued "Lenoir collects and stores data in its buffer. According to Lenioir, its watermark detector processes the data stored in the buffer. However, to do that, presumably the watermark detector must still receive data in order to process it. The data stored in Lenior buffer has not been received by the Lenior's watermark detector. Therefore, Lenoir fails to teach "observing and determining a location in a processor-readable memory ...where [the watermark detector] receives a subject input stream."

Lenior teaches the watermark detector 4 typically collects some video or audio material in buffer 5, performs some signal processing on this buffer 5 which adequate to meet the claimed limitation "observing and determining a location (i.e. buffer) where the detector receives a subject input stream (i.e. detector collects some video or audio material in buffer 5, performs processing on the buffer). Therefore, Lenior teaches observing and determining (i.e. a hacker could try to destroy or manipulate results

stored in buffer) in a processor-readable memory (buffer 5), where watermark detector receives a subject input stream (i.e. watermark detector receives and collects video or audio material) to perform detection if the stream has an embedded-signal. (i.e. signal processing on the buffer)

Applicant argued that Cox fails to list any attack or transformation of the watermark that teaches of suggests the claimed "intervening with clear reception of the subject input stream ...hindering watermark detection by the detector."

First, according to the American Heritage dictionary "intervening" is defined "to come, appear, occur, or lie between two things or two points of time." The broadest reasonable interpretation of "intervening with the clear reception of the subject input stream,... hindering watermark detection by the watermark detector" is anything that is interfering between clear reception of the subject input that hinders watermark detection by the detector. Second, Cox teaches some general methods for tampering with watermarks and describes a variety of possible attacks including attacks by affine transformation, attacks by noise addition, attacks by digital compression, exploiting the presence of a watermark detector device, attacks based on the presence of a watermark inserter, attacks by statistical averaging, and attacks on the copy control mechanism. Therefore, Cox teaches "intervening with the clear reception of the subject input stream" (i.e. an attacker may not have precise knowledge of the watermark. Nevertheless, he usually has access to a detector and the detector provides information about whether a certain piece of content contains a watermark or not. An attacker may not wish to remove the vary watermark that the content owner has embedded, which

may have been adapted according to a particular perceptual model. He only desires to extract a pattern that cancels the effect that the present watermark has on the detector. (see pages 7-13; Signal Transformation and Intentional Attacks)

Therefore, the previous rejection has been maintained.

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 1, 3-7, 46, 49 and 52 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1, 3-7, 46, 49 and 52 recite "a computer-readable storage medium" wherein the computer-readable storage medium is not explicitly defined to be limited to the statutory subject matter. Therefore, claims 1, 3-7, 46, 49 and 52 read in light of the specification includes a non-statutory subject matter.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 4-9, 12-18, 20-22 and 48-52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lenoir et al. (hereinafter Lenoir) US 6,671,806 in view of Cox et al. "Some general methods for tampering with watermarks" IEEE , 1998, pages 1-15.

As per claims 1, 8-9 and 16-17:

Lenoir teaches observing and determining a location in a processor-readable memory of a computer, where a dynamic embedded-signal detection program module ("watermark detector") receives a subject input stream for the watermark detector to perform detection thereon to determine if the stream has an embedded-signal therein. (col. 1, lines 55-65; col.4, lines 2-18)

Lenoir does not explicitly disclose intervening with clear reception of the subject input stream, thereby hindering watermark detection by the watermark detector. Cox in analogous art, however, teaches intervening with clear reception of the subject input stream, thereby hindering detection by the detector. (5. Signal Transformation; 6. Intentional Attack) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the system disclosed by Lenoir with Cox in order to examine to what extent a watermark can be resistant to tampering to a variety of possible attacks. (Cox Abstract)

As per claim 18:

The combination of Lenoir and Cox teaches all the subject matter as discussed above. In addition, Lenoir further teaches wherein the watermark-detector detector is further configured to detect and observe the watermark detector in a processor-

readable memory of a computer to determine its location in such memory. (col. 1, lines 55-65; col.4, lines 2-18)

As per claims 3, 11 and 19:

The combination of Lenoir and Cox teaches all the subject matter as discussed above. In addition Cox further teaches wherein the intervening comprises adjusting "play-rate" of the incoming stream. (5. Signal Transformation; 6. Intentional Attack)

As per claim 4-5, 12-13 and 20:

The combination of Lenoir and Cox teaches all the subject matter as discussed above. In addition, Cox further discloses wherein the intervening comprises introducing a countersignal into the incoming stream. (5. Signal Transformation; 6. Intentional Attack)

As per claim 6, 14 and 21:

The combination of Lenoir and Cox teaches all the subject matter as discussed above. In addition Cox further teaches maintaining the intervening while the input stream is being consumed. (5. Signal Transformation; 6. Intentional Attack)

As per claims 7, 15 and 22:

The combination of Lenoir and Cox teaches all the subject matter as discussed above. In addition Cox further teaches wherein the type of the subject input stream is selected from a group consisting of image, audio, video, multimedia, software, metadata, and data. (5. Signal Transformation; 6. Intentional Attack)

As per claims 52:

Lenoir teaches a method of facilitating circumvention of dynamic, robust, embedded-signal detection, the method comprising: determining where, in memory, a dynamic embedded-signal detection program module ("dynamic detector") in a processor-readable memory of a computer configured to dynamically detect watermarks in an input stream, based upon the observing the dynamic detector receives a subject incoming stream for the dynamic detector to perform embedded-signal detection thereon to determine if the subject incoming stream has an embedded-signal therein. (col. 1, lines 55-65; col.4, lines 2-18)

Lenoir does not explicitly disclose intervening with clear reception of the subject incoming stream, thereby hindering embedded-signal detection by the dynamic detector, wherein the intervening comprises adjusting "consumption-rate" of the incoming stream. Cox in analogous art, however, teaches intervening with clear reception of the subject incoming stream, thereby hindering embedded-signal detection by the dynamic detector, maintaining the intervening while the subject input stream is being played. (5. Signal Transformatio00n and 6. Intentional attacks) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the system disclosed by Lenoir with Cox in order to examine to what extent a watermark can be resistant to tampering to a variety of possible attacks. (Cox Abstract)

As per claims 48:

Lenoir teaches a system for facilitating circumvention of dynamic, robust, embedded-signal detection, the system comprising: a memory-location determiner ("watermark-detector detector") configured to determine where, in a memory, an

embedded-signal detection program module ("detector") receives a subject input stream for the detector to perform detection thereon to determine if the subject input stream has an embedded-signal therein and further configured to detect and observe the detector in a processor-readable memory of a computer to determine its location in such memory. (col. 1, lines 55-65; col.4, lines 2-18)

Lenoir fails to explicitly disclose an intervener configured to intervene with clear reception of the subject input stream, thereby hindering detection by the detector, wherein the intervening comprises adjusting the incoming rate for the input stream. Cox in analogous art, however, teaches an intervener configured to intervene with clear reception of the subject input stream, thereby hindering detection by the detector, wherein the intervening comprises adjusting the incoming rate for the input stream. (5. Signal Transformation and 6. Intentional attacks) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the system disclosed by Lenoir with Cox in order to examine to what extent a watermark can be resistant to tampering to a variety of possible attacks. (Cox Abstract)

As per claims 49 and 50-51:

Lenoir teaches a computer-readable storage medium having computer-executable instructions that, when executed by a computer, performs a method for facilitating circumvention of watermark detection, the method comprising: determining where, in a memory, a dynamic watermark detection program module ("watermark detector") receives a subject input stream for the watermark detector to perform watermark detection thereon to determine if the subject input stream has an embedded-

signal therein; observing and determining a location in a processor-readable memory of a computer the detector receives an input stream. (col. 1, lines 55-65; col.4, lines 2-18)

Lenoir fails to explicitly disclose intervening with clear reception of the subject input stream, thereby hindering watermark detection by the watermark detector, wherein the intervening comprises introducing a countersignal, the countersignal modifying the reception by introducing a noise countersignal. Cox in analogous art, however, teaches intervening with clear reception of the subject input stream, thereby hindering watermark detection by the watermark detector, wherein the intervening comprises introducing a countersignal, the countersignal modifying the reception by introducing a noise countersignal. (5. Signal Transformation and 6. Intentional attacks) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the system disclosed by Lenoir with Cox in order to examine to what extent a watermark can be resistant to tampering to a variety of possible attacks. (Cox Abstract)

1. Claims 3, 11, 19, 46-47 and 53-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lenoir et al. (hereinafter Lenoir) US 6,671,806 in view of Cox et al. "Some general methods for tampering with watermarks" IEEE, 1998, pages 1-15 and further in view of Tobias et al. WO 01/24530 (hereinafter Tobias).

As per claims 3, 11 and 19:

The combination of Lenoir and Cox teaches all the subject matter as discussed above. None of the prior art explicitly disclose wherein the intervening comprises adjusting "play-rate" of the incoming stream. Tobias in analogous art, however, teaches

wherein the intervening comprises adjusting "play-rate" of the incoming stream. (page 3, Summary of the Invention) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the system disclosed by Lenoir and Cox with Tobias in order to encode streaming media by generating a plurality of versions of the digital content. (Abstract; Tobias)

As per claims 46 and 53:

Lenoir teaches a computer-readable storage medium having computer-executable instructions that, when executed by a computer, performs a method for facilitating circumvention of watermark detection, the method comprising: determining where, in a processor-readable memory, a dynamic watermark detection program module ("watermark detector") receives a subject input stream for the watermark detector to perform watermark detection thereon to determine if the subject input stream has a watermark therein; and observing and determining a location in a processor-readable memory of a computer the detector receives an input stream. Rhoads in analogous art, however, discloses observing and determining a location in a processor-readable memory of a computer the detector receives an input stream. (col. 1, lines 55-65; col.4, lines 2-18)

Lenoir fails to explicitly disclose intervening with clear reception of the subject input stream, thereby hindering detection by the watermark detector, wherein the intervening comprises adjusting "play-rate" of the input stream. Cox in analogous art, however, teaches intervening with clear reception of the subject input stream, thereby hindering detection by the watermark detector. (5. Signal Transformation and 6.

Intentional attacks) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the system disclosed by Lenoir with Cox in order to examine to what extent a watermark can be resistant to tampering to a variety of possible attacks. (Cox Abstract)

Both references do not explicitly disclose wherein the intervening comprises adjusting "play-rate" of the incoming stream. Tobias in analogous art, however, teaches wherein the intervening comprises adjusting "play-rate" of the incoming stream. (page 3, Summary of the Invention) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the system disclosed by Lenoir and Cox with Tobias in order to encode streaming media by generating a plurality of versions of the digital content. (Abstract; Tobias)

As per claims 47 and 54:

Lenoir teaches a method of facilitate circumvention of dynamic, robust, embedded signal detection, the method comprising: observing a dynamic embedded-signal detection program module ("dynamic detector) in a processor-readable memory of a computer configured to dynamically detect watermarks in an input stream, based upon observing, determining a location in a processor-readable memory, the location being where the dynamic detector receives a subject incoming stream for the dynamic detector to perform embedded-signal detection thereon to determine if the subject incoming stream has an embedded-signal therein. (col. 1, lines 55-65; col.4, lines 2-18)

Lenoir fails to explicitly disclose intervening with clear reception of the subject input stream, thereby hindering detection by the watermark detector, wherein the

intervening comprises adjusting "consumption-rate" of the input stream. Cox in analogous art, however, teaches intervening with clear reception of the subject input stream, thereby hindering detection by the watermark detector. (5. Signal Transformation and 6. Intentional attacks) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the system disclosed by Lenoir with Cox in order to examine to what extent a watermark can be resistant to tampering to a variety of possible attacks. (Cox Abstract)

Both references do not explicitly disclose wherein the intervening comprises adjusting "consumption-rate" of the incoming stream. Tobias in analogous art, however, teaches wherein the intervening comprises adjusting "consumption-rate" of the incoming stream. (page 3, Summary of the Invention;) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the system disclosed by Lenioir and Cox with Tobias in order to encode streaming media by generating a plurality of versions of the digital content. (Abstract; Tobias)

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHEWAYE GELAGAY whose telephone number is (571)272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Shewaye Gelagay/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437